МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«Национальный исследовательский ядерный университет «МИФИ»

Снежинский физико-технический институт –
филиал федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский ядерный университет «МИФИ»
(СФТИ НИЯУ МИФИ)

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 0BDE66000DAECEA44E1BF4E83F4BE9DB
Владелец: НИЯУ МИФИ
Действителен: с 29.12.2021 до 29.12.2022

«УТВЕРЖДАЮ»
Зам. руководителя по учебной
и научно-методической работе
П. О. Румянцев
«_____»_____ 2020 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЗАЩИТА ИНФОРМАЦИИ
наименование дисциплины

Направление подготовки ____01.04.02 «Прикладная математика и информатика»

Профиль подготовки «Математическое моделирование и высокопроизводительные вычисления и технологии»

Наименование образовательной программы:_____

Квалификация (степень) выпускника: магистр
(бакалавр, магистр, специалист)

Формаобучения_____очная_____
(очная, очно-заочная (вечерняя), заочная)

г. Снежинск, 2020 г.

1. ЦЕЛИ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Целями освоения учебной дисциплины __*Защита информации*__ является подготовки выпускников к научно-исследовательской работе, а также для подготовки специалистов, способных решать разнообразные теоретические и практические задачи, возникающие при передаче и хранении информации

2. МЕСТО УЧЕБНОЙ ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВПО

Дисциплина «Математические методы и программное обеспечение защиты информации» относится к профессиональному циклу. Для изучения данной учебной дисциплины необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами: математический анализ, алгебра и геометрия, дифференциальные уравнения, устойчивость и стабилизация линейных систем, математические модели в естествознании и методы их исследования.

3. КОМПЕТЕНЦИИ СТУДЕНТА, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ / ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ ОБРАЗОВАНИЯ И КОМПЕТЕНЦИИ СТУДЕНТА ПО ЗАВЕРШЕНИИ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

ПК-1	способностью проводить научные исследования и получать новые научные и прикладные результаты самостоятельно и в составе научного коллектива
ПК-2	способностью разрабатывать концептуальные и теоретические модели решаемых научных проблем и задач
ПК-3	способностью углубленного анализа проблем, постановки и обоснования задач научной и проектно-технологической деятельности
ПК-4	способностью разрабатывать концептуальные и теоретические модели решаемых задач проектной и производственно-технологической деятельности
ПСК-1	способность к развитию инновационного потенциала новых научных и научно-технологических разработок по профилю профессиональной деятельности, а также готовность к проведению экспертизы инновационных проектов в сфере своей профессиональной деятельности
ПСК-2	способность к разработке и внедрению прикладного программного обеспечения, способствующего решению передовых задач науки и техники

4. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Семестр	Трудоем-кость, кредит	Общий объем курса, час.	Лекции, час.	Практич. занятия, час.	КСР, час.	СРС, час.	Форма контроля, Экз./зачет
3	4	144	20	10	0	114	зачет

Занятия в интерактивной форме составляют 17 часов от общего объёма аудиторных занятий. Общая трудоемкость дисциплины составляет ___4___ кредитов, ___144_____ часов.

№ п/п	Раздел учебной дисциплины	Недели	Виды учебной деятельности, включая самостоятельную работу студентов и трудоемкость (в часах)	Аттестация раздела *(неделя, форма)*	Текущий контроль успеваемости *(неделя, форма)*	Максимальный балл за раздел *

			Лекции	Практ. занятия/ семинары	КСР			
3 семестр								
1	Введение	1	2	-				5
2	Принципы обеспечения защиты информации. Уровни информационной защиты	2	2	1				5
3	Криптографические системы и криптоанализ	3	2	2				5
4	Технические аспекты обеспечения защиты информации	4-5	4	2				5
5	Атаки системы снаружи и изнутри	6-7	4	2				5
6	Основные направления работ по созданию систем комплексной защиты информационной системы объекта (предприятия)	8-10	4	2				5
7	Мобильные программы	11	1	1				5
8	Заключение	12	1	-				15
Всего:			20	10	-	-	-	50
	Экзамен							50
	Итого за 1 семестр:							100

При сдаче отчетов и письменных работ проводится устное собеседование.

4.2. Содержание разделов дисциплины

1. Введение

Основные понятия защиты информации. Роль и место конфиденциальной информации в обеспечении безопасности Российской Федерации.

Общие принципы обеспечения информационной безопасности объекта (предприятия). Структура дисциплины.

2. Принципы обеспечения защиты информации. Уровни информационной защиты

Классификация и источники наиболее распространенных угроз информационной безопасности.

Анализ уязвимости информационных систем. Классификация сетевых атак.

Безопасность локальных вычислительных сетей и интегрированных информационных систем управления.

Распределенное хранение файлов. Оценка рисков.

Требования по обеспечению информационной безопасности информационной системы. Уровни информационной защиты.
Знаменитые дефекты системы безопасности UNIX, TENEX, OS/360.
Принципы проектирования систем безопасности.

3. Криптографические системы и криптоанализ

Криптология. Криптосистемы. Понятие стойкости криптографического алгоритма. Анализ надежности криптосистем.
Классические методы криптоанализа. Архитектура систем защиты данных.

4. Технические аспекты обеспечения защиты информации

Методы реализации программно-технического уровня защиты информационных систем.
Программно - аппаратные средства комплексной защиты информации.
Подсистема идентификации и аутентификации. Подсистема управления доступом. Подсистема протоколирования аудита.
Конфиденциальность и целостность данных и сообщений. Контроль участников взаимодействия.
Излечения элементов ПЭВМ. Экранирование помещений, предназначенных для размещения ПЭВМ и технических средств обработки информации.

5. Атаки системы снаружи и изнутри

Основные характеристики технических средств защиты от несанкционированного доступа.
Требования по защите информации от несанкционированного доступа для автоматизированных систем защиты третьей, второй и первой групп. Требования по защите информации от несанкционированного доступа для средств вычислительной техники. Требования к межсетевым экранам.

6. Основные направления работ по созданию систем комплексной защиты информационной системы объекта (предприятия)

Организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием.
Классификация интегрированных информационных систем управления предприятием.
Система компьютерной безопасности. Оснащение объекта техническими средствами противодействия экономическому шпионажу и защиты речевой информации.
Этапы проведения работ по обеспечению информационной безопасности предприятия.

7. Мобильные программы

Мобильные программы, апплеты. Примеры. Метод «песочницы». Интерпретируемые программы. Программы с подписями. Примеры систем безопасности. Безопасность в системе Java.

8. Заключение

Документы, регламентирующие деятельность по обеспечению защиты информации. Политика информационной безопасности Российской Федерации. Законы РФ в области информационной безопасности.
Проблемные вопросы. Перспективы развития. Исследования в области безопасности.
Рекомендации по дальнейшему овладению дисциплиной «Информационная безопасность и защита информации».

4.3 Содержание (темы) практических занятий

Раздел 2. Принципы обеспечения защиты информации. Уровни информационной защиты

1. 2.2. Системы безопасности и их дефекты

Раздел 3. Криптографические системы и криптоанализ

2. 3.1. Основы криптографии
3. 3.2. Шифрование с секретным ключом
4. 3.3. Шифрование с открытым ключом

Раздел 4. Технические аспекты обеспечения защиты информации

5. 4.1. Аутентификация пользователей
6. 4.3. Совершенствование безопасности паролей

Раздел 6. Основные направления работ по созданию систем комплексной защиты информационной системы объекта (предприятия)

7. 6.2. Перечни возможностей

Раздел 7. Мобильные программы

8. 7.3. Программы с подписями

Образовательные технологии

При освоении дисциплины используются следующие сочетания видов учебной работы с методами и формами активизации познавательной деятельности магистрантов для достижения запланированных результатов обучения и формирования компетенций.

Методы и формы активизации деятельности	**Виды учебной деятельности**			
	ЛК	Семинар	ЛБ	СРС
Дискуссия	х	х		
IT-методы	х		х	х
Командная работа		х	х	х
Разбор кейсов		х		
Опережающая СРС	х	х	х	х
Индивидуальное обучение			х	х
Проблемное обучение		х	х	х
Обучение на основе опыта		х	х	х

Для достижения поставленных целей преподавания дисциплины реализуются следующие средства, способы и организационные мероприятия:

- изучение теоретического материала дисциплины на лекциях с использованием компьютерных технологий;
- самостоятельное изучение теоретического материала дисциплины с использованием *Internet*-ресурсов, информационных баз, методических разработок, специальной учебной и научной литературы;
- закрепление теоретического материала при проведении лабораторных работ с использованием учебного и научного оборудования и приборов, выполнения проблемно-ориентированных, поисковых, творческих заданий.

6. Организация и учебно-методическое обеспечение самостоятельной работы студентов (СРС)

6.1. Текущая и опережающая СРС, направленная на углубление и закрепление знаний, а также развитие практических умений заключается в:

- работе магистрантов с лекционным материалом, поиск и анализ литературы и электронных источников информации по заданной проблеме и выбранной теме магистерской диссертации;
- поиске и анализе литературы и электронных источников информации по заданной проблеме и выбранной теме курсовой работы;
- переводе материалов из тематических информационных ресурсов с иностранных языков;
- изучении тем, вынесенных на самостоятельную проработку;
- изучении теоретического материала к лабораторным занятиям;
- подготовке и защите курсовой работы;
- подготовке к экзамену.

6.1.1. Темы, выносимые на самостоятельную проработку:

- история развития вычислительной техники за рубежом (США и Европа);
- история развития программного обеспечения за рубежом (США и Европа);
- современные методологии и информационные технологии, применяемые в области математического моделирования;
- системный подход к анализу и решению проблем, возникающих в процессе математического моделирования;
- учет специфики при моделировании открытых систем (синергия, самоорганизация).

6.2. Творческая проблемно-ориентированная самостоятельная работа (ТСР) направлена на развитие интеллектуальных умений, комплекса универсальных (общекультурных) и профессиональных компетенций, повышение творческого потенциала магистрантов и заключается в:

- поиске, анализе, структурировании и презентации информации, анализе научных публикаций по определенной теме исследований;
- анализе статистических и фактических материалов по заданной теме, проведении расчетов, составлении схем и моделей на основе статистических материалов;
- выполнении расчетно-графических работ;
- исследовательской работе и участии в научных студенческих конференциях, семинарах и олимпиадах.

7. Средства текущей и итоговой оценки качества освоения дисциплины (фонд оценочных средств)

Оценка успеваемости магистрантов осуществляется по результатам:

- самостоятельного (под контролем учебного мастера) выполнения лабораторной работы;
- взаимного рецензирования магистрантами работ друг друга;
- промежуточный анализ подготовленных магистрантами курсовых работ;
- устного опроса при сдаче выполненных индивидуальных заданий, защите отчетов по лабораторным работам и во время экзамена в первом семестре (для выявления знания и понимания теоретического материала дисциплины).

8. Учебно-методическое и информационное обеспечение дисциплины

а) **основная литература**:

- Партыка Т.Л., Попов И.И. Операционные системы, среды и оболочки: учебное пособие. – 5-е изд., перераб. и доп.– М.: ФОРУМ: ИНФРА-М, 2014 – 560 с.

б) дополнительная литература:

- Девянин П.Н. Модели безопасности компьютерных систем.– М.: ACADEMIA, 2005 – 144 с.
- Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах.– М.: ФОРУМ, 2010 – 368 с.
- Куприянов А.И., Сахаров А.В., Шевцов В.А. Основы защиты информации.– М.: Академия, 2006. – 256с.

в) программное обеспечение и Интернет-ресурсы:

http://ibooks.ru/
http://e.lanbook.com/
http://www.biblio-online.ru/home;jsessionid=2e1f56dad5e63541356653818b3d?0
http://kuperbook.biblioclub.ru/
http://www.studentlibrary.ru/
http://libcatalog.mephi.ru/cgi/irbis64r/cgiirbis_64.exe?C21COM=F&I21DBN=BOOK&P21DBN=BOOK

ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы в рамках курса предусмотрено использование следующих образовательных технологий:

1. Разбор задач и поиск их решения, доказательство формул и теорем. Занятия проводятся в интерактивной форме общения студентов между собой при поиске метода решения поставленной задачи и оформлении решения. Преподаватель обеспечивает консультационное сопровождение процесса поиска решения.

2. Вводная и обзорная лекции проводятся с применением мультимедийных средств обучения в виде презентации PowerPoint, с целью в наиболее сжатом концентрированном виде сделать обзор пройденного материала с указанием взаимосвязи между разделами дисциплины, освещением основных изученных подразделов, а также для формирования у студентов общего представления о месте дисциплины в общем перечне дисциплин ООП ВПО 01.04.02 «Прикладная математика и информатика» и о формируемых этой дисциплиной компетенциях.

3. Домашние задания выдаются преподавателем каждому студенту на каждом практическом занятии. Задание представляет собой номера задач и упражнений из сборника задач. Домашние задания сдаются преподавателю на проверку. Защита домашних заданий предусмотрена. Приём заданий возможен как в рукописном, так и в печатном виде.

4. Один раз в две недели преподавателем проводится текущая консультация. Вопросы можно задавать лично преподавателю в назначенное время.

1. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ.

Самостоятельная работа студентов составляет 79,17% от общего объёма занятий, предусмотренных рабочим учебным планом направления подготовки 01.04.02 «Прикладная математика и информатика» – 114 часа.

Часы на самостоятельную работу распределяются равномерно на весь курс обучения. Разделы, выводимые на самостоятельное изучение в рамках лекционных и практических разделов, устанавливаются преподавателем на каждой неделе, в зависимости от скорости усвоения материала студентами. Темы для самостоятельного изучения оглашаются преподавателем в конце каждого занятия и заносятся студентами в график самостоятельной работы.

Текущий контроль успеваемости проводится посредством проверки домашних заданий и конспекта текущей лекции.

Аттестация раздела проводится в виде контрольной работы. Максимальный балл за каждый раздел установлен п.4. настоящей рабочей программы.

2. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

Мультимедийная аудитория (Л-318). Компьютерный класс, оснащённый компьютерами с выходом в Интернет, а также принтером, сканером, ксероксом:

- Core Dual 2,4 МГц (2009 г.) - 15 шт.
- Принтер HP LJ P3005 DN (2009 г.) - 1 шт.
- Сканер HP SJ 4370 – 1 шт.
- Ноутбук Samsung (2008)
- Проектор ASER X1260 (2008)

9. Фонды оценочных средств.

Перечень тем рефератов по дисциплине:

1 Угрозы информационной безопасности предприятия (организации) и способы борьбы с ними
2 Современные средства защиты информации
3 Современные системы компьютерной безопасности
4 Современные средства противодействия экономическому шпионажу
5 Современные криптографические системы
6 Криптоанализ, современное состояние
7 Правовые основы защиты информации
8 Технические аспекты обеспечения защиты информации. Современное состояние
9 Атаки на систему безопасности и современные методы защиты
10 Современные пути решения проблемы информационной безопасности РФ

Вопросы для подготовки к зачету:

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности Российской Федерации существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?
8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10. Какими способами снизить угрозу сниффинга пакетов?
11. Какие меры по устранению угрозы IP-спуфинга существуют?
12. Что включает борьба с атаками на уровне приложений?
13. Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14. В чем заключается распределенное хранение файлов?
15. Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16. Какие уровни информационной защиты существуют, их основные составляющие?
17. В чем заключаются задачи криптографии?
18. Зачем нужны ключи?
19. Какая схема шифрования называется многоалфавитной подстановкой?
20. Какие системы шифрования вы знаете?
21. Что включает в себя защита информации от несанкционированного доступа?
22. В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23. Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24. Какие задачи выполняет подсистема управления доступом?

25. Какие требования предъявляются к подсистеме протоколирования аудита?
26. Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27. В чем заключается контроль участников взаимодействия?
28. Какие функции выполняет служба регистрации и наблюдения?
29. Что такое информационно-опасные сигналы, их основные параметры?
30. Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
31. Какой процесс называется аутентификацией пользователя?
32. Какие схемы аутентификации вы знаете?
33. Что такое смарт-карты?
34. Какие требования предъявляются к современным криптографическим системам защиты информации?
35. Что такое симметричная криптосистема?
36. Какие виды симметричных криптосистем существуют?
37. Что такое асимметричная криптосистема?
38. Что понимается под односторонней функцией?
39. Как классифицируются криптографические алгоритмы по стойкости?
40. В чем заключается анализ надежности криптосистем?
41. Что такое дифференциальный криптоанализ?
42. В чем сущность криптоанализа со связанными ключами?
43. В чем сущность линейного криптоанализа?
44. Какие атаки изнутри вы знаете?
45. Какая программа называется логической бомбой?
46. Какими способами можно проверить систему безопасности?
47. Что является основными характеристиками технических средств защиты информации?
48. Какие требования предъявляются к автоматизированным системам защиты третьей группы?
49. Какие требования предъявляются к автоматизированным системам защиты второй группы?
50. Какие требования предъявляются к автоматизированным системам защиты первой группы?
51. Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
52. Какие требования предъявляются к межсетевым экранам?
53. Какие имеются показатели защищенности межсетевых экранов?
54. Какие атаки системы снаружи вы знаете?
55. Какая программа называется вирусом?
56. Какая атака называется атакой отказа в обслуживании?
57. Какие виды вирусов вы знаете?
58. Какие вирусы называются паразитическими?
59. Как распространяются вирусы?
60. Какие методы обнаружения вирусов вы знаете?
61. Какая программа называется монитором обращения?
62. Что представляет собой домен?
63. Как осуществляется защита при помощи ACL-списков?
64. Какой список называется перечнем возможностей?
65. Какие способы защиты перечней возможностей вы знаете?
66. Из чего состоит высоконадежная вычислительная база (TCB)?

67. Какие модели многоуровневой защиты вы знаете?

68. В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?

69. Какие характеристики положены в основу системы классификации информационных систем управления предприятием?

70. Какие задачи решает система компьютерной безопасности?

71. Какие пути защиты информации в локальной сети существуют?

72. Какие задачи решают технические средства противодействия экономическому шпионажу?

73. Какой порядок организации системы видеонаблюдения?

74. Что включает в себя защита информационных систем с помощью планирования?

75. Какие условия работы оцениваются при планировании?

76. Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?

77. Что такое мобильные программы?

78. Что такое концепция потоков?

79. Что представляет собой метод «Песочниц»?

80. Что такое интерпретация?

81. Что такое программы с подписями?

82. Что представляет собой безопасность в системе Java?

83. Назовите несколько примеров политик безопасности пакета JDK 1.2?

84. Какие международные документы регламентируют деятельность по обеспечению защиты информации?

85. Что понимают под политикой информационной безопасности?

86. Что включает в себя политика информационной безопасности РФ?

87. Какие нормативные документы РФ определяют концепцию защиты информации?

Программа составлена в соответствии с требованиями ФГОС ВПО по направлению подготовки 01.04.02 «Прикладная математика и информатика», ОС ВО НИЯУ МИФИ протокол № 13/06 от 07.11.2013 г.

Автор: доцент кафедры АИВС, к.т.н., Крушный Валерий Васильевич

Рецензент_____

Программа одобрена на заседании кафедры АИВС 29 июня 2020 г., протокол №